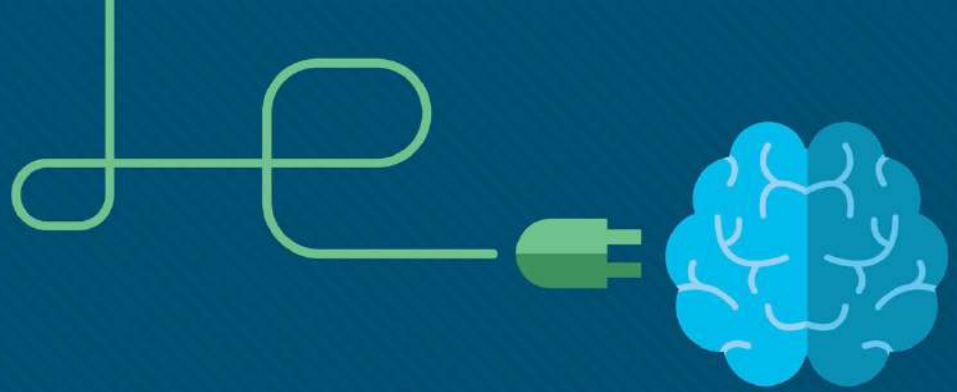


Capítulo 3: Proteção de seus dados e privacidade

Introdução ao Cybersecurity v2.1

Parte 3.1 Como proteger os dados

Proteger seus dispositivos de computação

- Manter o Firewall habilitado
  - Impedir o acesso não autorizado aos seus dados ou dispositivos de computação
  - Manter o firewall atualizado
- Usar antivírus e antispyware
  - Impedir o acesso não autorizado aos seus dados ou dispositivos de computação
  - Somente baixar o software de sites confiáveis
  - Manter o software atualizado
- Gerenciar o seu sistema operacional e navegador
  - Definir as configurações de segurança para média ou superior
  - Atualizar o sistema operacional do seu computador e navegador
  - Baixar e instalar os patches de software mais recentes e atualizações de segurança
- Proteger todos os seus dispositivos
  - Proteger com senha
  - Criptografar os dados
  - Só armazenar as informações necessárias
  - Dispositivos de IoT

Usar redes sem fio com segurança

- Rede sem fio domiciliar
  - Altere o SSID predefinido e a senha administrativa padrão no seu roteador WiFi.
  - Desative a transmissão de SSID
  - Use o atributo de criptografia WPA2
  - Esteja atento à falha de segurança de protocolo WPA2 – KRACK
    - Permite que o intruso quebre a criptografia entre roteador sem fio e clientes
- Tenha cuidado ao usar hotspots de WiFi públicos
  - Evite o acesso ou envio de informações confidenciais
  - O uso do túnel VPN pode evitar invasões
- Desative o Bluetooth quando ele não estiver em uso

Use senhas exclusivas para cada conta on-line

- Impede que os criminosos acessem todas as suas contas on-line usando credenciais roubadas
- Use gerenciadores de senha para ajudar a lembrar das senhas
- Dicas para escolher uma boa senha:
  - Não use palavras do dicionário ou nomes em qualquer idioma
  - Não use erros ortográficos comuns de palavras do dicionário
  - Não use nomes de computador ou de contas
  - Se possível use caracteres especiais, como! @ # $ % ^ & * ( )
  - Use uma senha com 10 ou mais caracteres

OK	Good	Melhorou
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

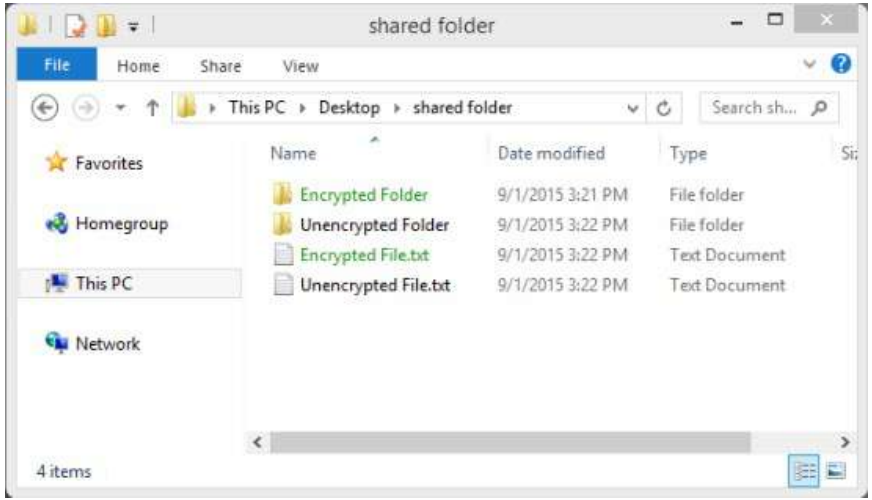
Usar a frase secreta, em vez de uma senha

- Dicas para escolher uma boa senha:
  - Escolha uma frase significativa para você
  - Adicione caracteres especiais, como ! @ # $ % ^ & * ( )
  - Quanto maior melhor
  - Evite frases comuns ou famosas, como a letra de uma música famosa
- Resumo das novas orientações da NIST:
  - No mínimo 8 caracteres e no máximo 64 caracteres
  - Não use senhas comuns e fáceis de ser descobertas, como a senha abc123
  - Não aplique regras de composição, como ter que incluir números e letras maiúsculas e minúsculas
  - Nenhuma autenticação baseada em conhecimento, como informações de perguntas secretas compartilhadas, dados comerciais e histórico de transações
  - Melhore a precisão da digitação, evitando que o usuário veja a senha durante a digitação
  - Todas os caracteres e espaços são permitidos
  - Não use dicas para senhas
  - Não aplique expiração de senha periódica ou arbitrária

OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Melhorou	Acat th@tlov3sd0gs.

Criptografar seus dados

- Dados criptografados só podem ser lidos com a chave secreta ou a senha
- Impede que usuários não autorizados leiam o conteúdo
- O que é criptografia?
  - processo de converter as informações em um formato que não pode ser lido por uma pessoa não autorizada.



Backup dos seus dados

- Evita a perda de dados insubstituíveis
- Precisa de local de armazenamento adicional para os dados
- Copia os dados para o local de backup de forma regular e automática
- Backup local
  - NAS, disco rígido externo, CDs/DVDs, pen drives ou fitas
  - Controle total e responsável pelo custo e manutenção
- Serviço de armazenamento em nuvem, tais como AWS
  - Acesso ao backup, contanto que você tenha acesso à sua conta
  - pode ser necessário ser mais seletivo sobre os dados de backup

Excluir os dados permanentemente

- Use as ferramentas disponíveis para excluir permanentemente: SDelete e Secure Empy Trash, por exemplo
- Destrua o dispositivo de armazenamento para garantir que os dados sejam irrecuperáveis
- Exclua as versões on-line

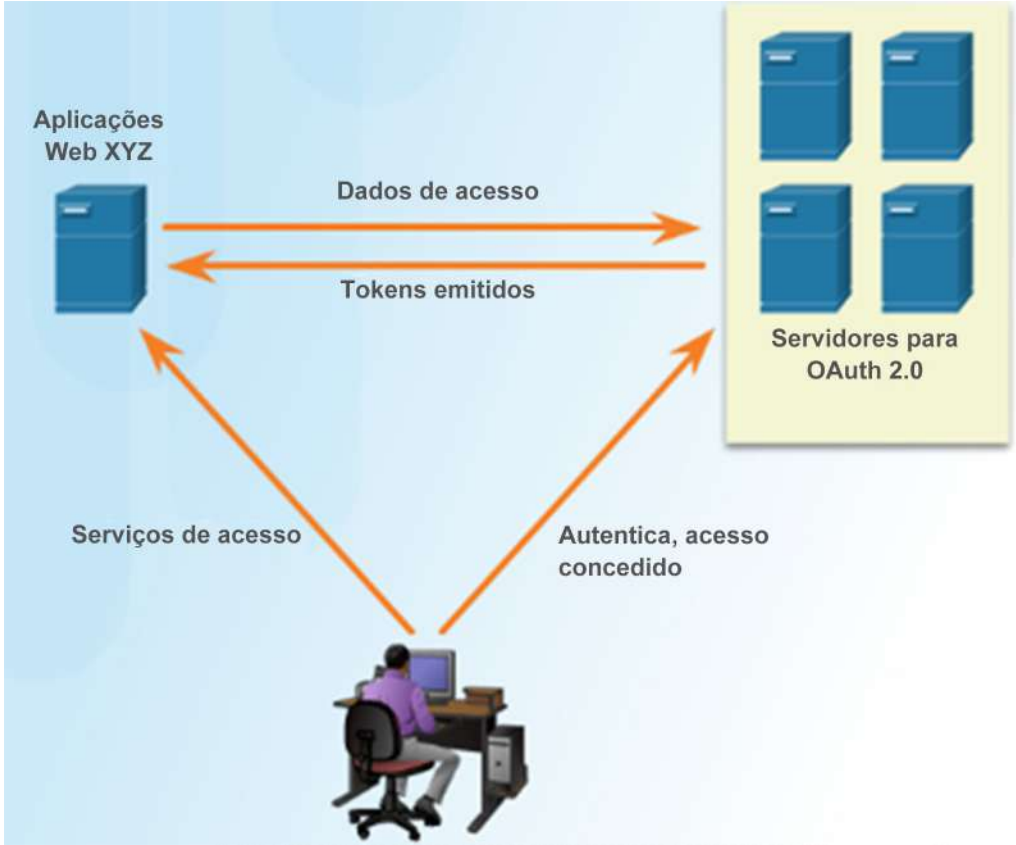
3.2 Como proteger a sua privacidade on-line

Autenticação de dois fatores

- Serviços on-line populares usam a autenticação de dois fatores
- É preciso nome de usuário/senha ou PIN e um segundo token para acesso:
  - **Objeto físico** – cartão de crédito, cartão de débito, telefone ou fob
  - **Verificação biométrica** – impressão digital, impressão palmar, facial ou reconhecimento de voz

OAuth 2.0

- Um protocolo padrão aberto que permite às credenciais de um usuário final acessarem aplicativos de terceiros sem expor a senha do usuário.
- Funciona como o intermediário para decidir se deseja permitir aos usuários finais o acesso a aplicativos de terceiros.



Não compartilhe muitas informações na mídia social

- Compartilhe o mínimo de informação possível na mídia social
- Não compartilhe informações tais como:
  - Data de nascimento
  - Endereço de e-mail
  - Telefone
- Verifique as suas configurações de mídia social

Acha que está compartilhando informações demais?

Privacidade de e-mail e navegador da Web

- Enviar um e-mail é como enviar um cartão postal.
- As cópias do e-mail podem ser lidas por qualquer pessoa com acesso.
- O e-mail passa por diferentes servidores
- Usar o modo de navegação privado pode impedir que outras pessoas obtenham as informações sobre suas atividades on-line.
- Modo privado no navegador popular
  - **Microsoft Internet Explorer**: InPrivate
  - **Google Chrome**: Incognito
  - **Mozilla Firefox**: Aba privada / janela privada
  - **Safari**: Privado: Navegação privada